RSAC 2025 Conference

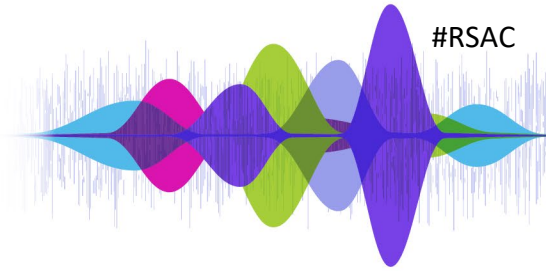
Many Voices.
One Community.

SESSION ID: FND-M06

From Good to Great, Foundations of Application Security

Shannon Lietz

CEO & Founder
Hackergirl



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

© 2025 Hackergirl. All Rights Reserved.

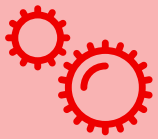
WHY ARE WE HERE?

PROBLEM

Software continues to adapt and grow to cover an almost infinite number of use cases on a continuous basis providing opportunities to make **software mistakes** that create **adversary opportunities**.

STRUGGLE

Understanding the software mistakes that create compliance gaps and lead to adversary threats requires **time**, specialized **skills**, and **tooling** to establish the foundation of application security which often prevent software developers from delivering quickly.



GOAL

Enabling effective and efficient application security that operates at the speed and scale of software delivery provides a competitive advantage for organizations by **enabling compliance** with requirements that establish an authority to operate while **preventing adversary opportunities** that disrupt business.

© 2025 Hackergirl. All Rights Reserved.

AGENDA

INTRODUCTION TO APPLICATION SECURITY

BASIC APPLICATION SECURITY

INTERMEDIATE APPLICATION SECURITY

ADVANCED APPLICATION SECURITY

Q&A

© 2025 Hackergirl. All Rights Reserved.

INTRODUCTION TO APPLICATION SECURITY

Understanding definitions, building blocks, and goals.

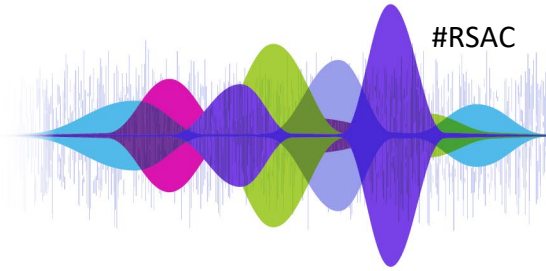
- What is the Software Dev Life Cycle?
- What is Application Security?
- What is the Scope of Application Security?
- What are the Top Frameworks?
- Good vs. Great Application Security
- What are the Foundations of Great AppSec?
- What are Foundational AppSec Controls?

© 2025 Hackergirl. All Rights Reserved.

WHAT IS SOFTWARE DEV LIFE CYCLE?

> "THE SOFTWARE DEVELOPMENT LIFE CYCLE IS A STRUCTURED PROCESS FOR PLANNING, DEVELOPING, TESTING, DEPLOYING, AND MAINTAINING SOFTWARE SYSTEMS TO ENSURE QUALITY APPLICATIONS."

© 2025 Hackergirl. All Rights Reserved.

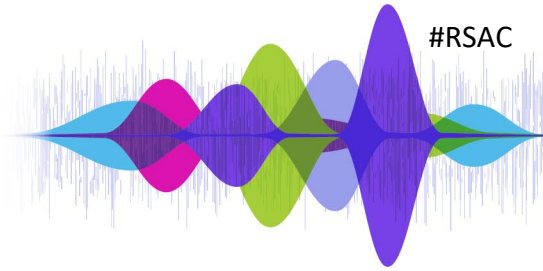


INTRODUCTION TO APPLICATION SECURITY

WHAT IS APPLICATION SECURITY?

> “APPLICATION SECURITY IS A SET OF SKILLS REQUIRED FOR PROVIDING THE CAPABILITIES THAT ENSURE AN APPLICATION MEETS ITS COMPLIANCE AND ADVERSARY RESILIENCE GOALS IN THE SOFTWARE DEV LIFE CYCLE.”

© 2025 Hackergirl. All Rights Reserved.



WHAT IS THE SCOPE OF APPLICATION SECURITY?

Web Applications

Interactive applications that run in a web browser, accessed through the internet.

Mobile Applications

Apps designed for smartphones and tablets, often with touch-based interfaces.

Desktop Applications

Software programs that run directly on a computer's operating system.

Enterprise Applications

Large-scale software systems used by organizations to manage business processes and data.

Embedded Applications

Software that is integrated into hardware devices, such as appliances or vehicles.

AI Applications

Software with AI-capabilities embedded to support users with complex needs.

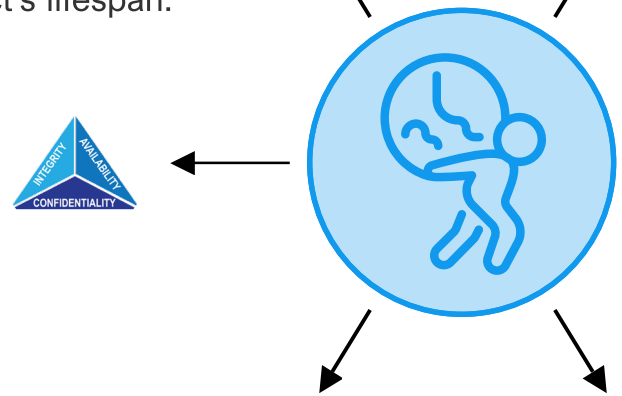
© 2025 Hackergirl. All Rights Reserved.

INTRODUCTION TO APPLICATION SECURITY

WHAT ARE THE TOP FRAMEWORKS?

The **SDLC (Software Development Life Cycle)** is a structured process that guides the development, testing, and deployment of software, ensuring quality, security, and efficiency throughout the project's lifespan.

The **CWE (Common Weakness Enumeration)** is a list of software security weaknesses which can lead to vulnerabilities, helping developers identify and mitigate these issues during the software development lifecycle.



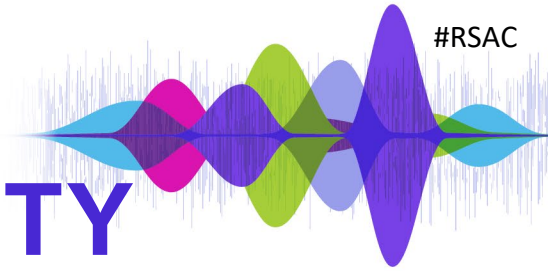
The **CIA Triad** is a fundamental security model that focuses on ensuring the Confidentiality, Integrity, and Availability of systems and data.

The **OWASP Top 10** is a widely recognized list of security risks to web applications, providing curated guidance and prioritization for developers to improve their applications.

NIST 800-218 provides guidelines for developing and maintaining secure software, focusing on integrating security practices throughout the software development life cycle

MITRE ATT&CK is a constantly evolving knowledge base of adversary tactics, techniques, and procedures, providing a standardized framework for understanding and mitigating cyber threats.

© 2025 Hackergirl. All Rights Reserved.



INTRODUCTION TO APPLICATION SECURITY

GOOD VS. GREAT APPLICATION SECURITY

GOOD

- ✓ Reactive Approach
- ✓ Basic Compliance Requirements
- ✓ Focused on Code Security
- ✓ Periodic Testing
- ✓ Vulnerability-centric Defenses
- ✓ Encryption At Rest and in Transit
- ✓ Assesses Risk of Libraries & Packages prior to deployment
- ✓ Reports on Vulnerabilities

GREAT

- ✓ **Adds Proactive Approach**
- ✓ **Adds Adversary Resilience Requirements**
- ✓ **Adds Configs and Business Logic**
- ✓ **Matures to Continuous Testing**
- ✓ **Adds Adversary Context**
- ✓ **Adds Application-Level Encryption**
- ✓ **Adds Assessment of Libraries & Packages on ingest**
- ✓ **Adds Metrics for Resilience**

© 2025 Hackergirl. All Rights Reserved.

INTRODUCTION TO APPLICATION SECURITY

WHAT ARE THE FOUNDATIONS OF GREAT APPSEC?

SKILLS

- Identify Adversaries
- Identify Threats
- Design a Secure App
- Build Secure Code
- Test Code
- Test App Flows
- Test Business Logic
- Identify Vulnerabilities
- Patch Vulnerabilities
- Identify Incidents
- Respond to Incidents

CAPABILITIES

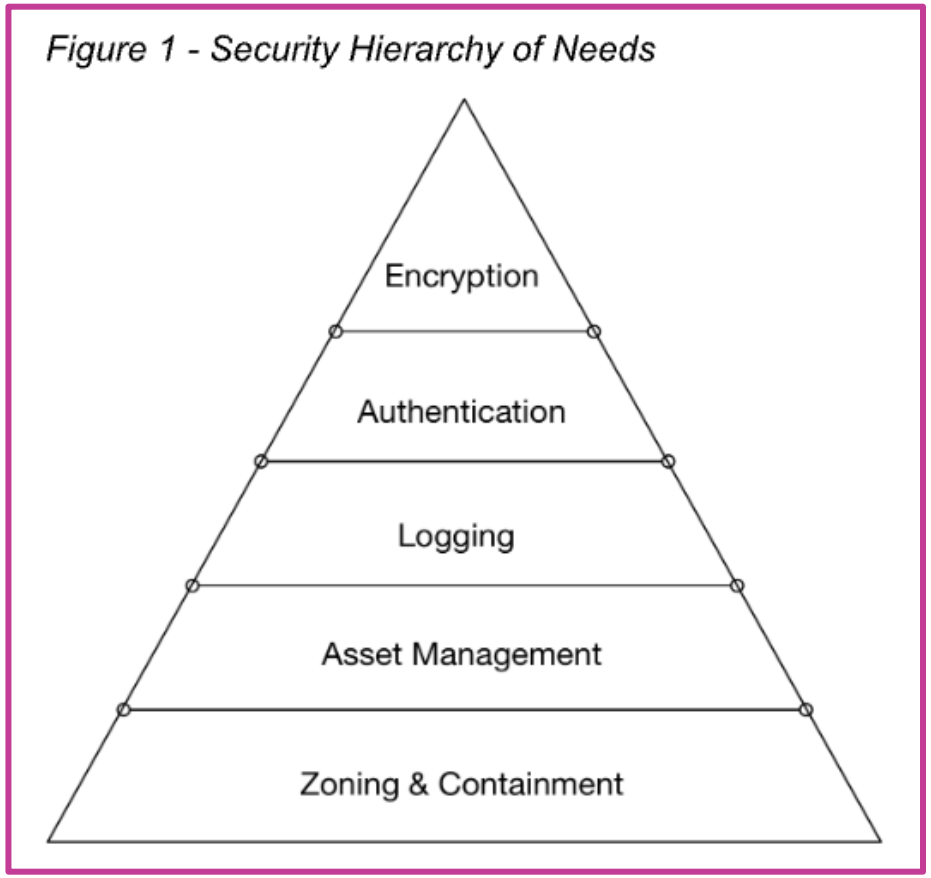
- Model Adversaries
- Model Threats
- Model Controls
- Test & Identify Weaknesses
  - Test Code for Security Defects (SAST, IAST
  - Test Components for Security Defects (SCA
  - Test Application for Security Defects (DAST)
- Mitigate Risks of Weaknesses
- Respond to Incidents

GOALS

- Trusted Brand
- Application Availability
- Data Integrity
- Data Confidentiality
- Data Privacy

© 2025 Hackergirl. All Rights Reserved.

WHAT ARE FOUNDATIONAL APPSEC CONTROLS?



- ✓ Encrypt for Privacy
- ✓ Identify & Authenticate
- ✓ Keep Secrets Safe
- ✓ Log and Alert on Mischief
- ✓ Don't Drift on Baseline Configs
- ✓ Validate Inputs & Outputs
- ✓ Segment for Safety

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

Respond and Remediate Quickly

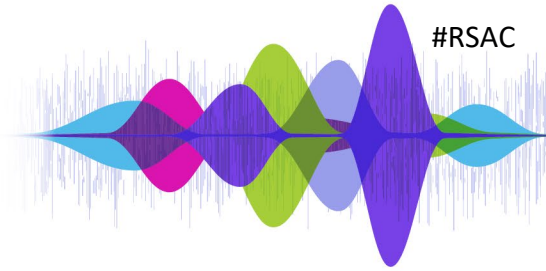
- What is the Goal of Basic AppSec?
- What are Key Metrics for Basic?
- What are Basic AppSec Processes?
- What is App Compliance & App Audit?
- What are App Disclosures & Incidents?
- How do I Enable App Auth & Logging?
- How do I Review an App with Developers?
- How do I Get Started with App Reviews?

© 2025 Hackergirl. All Rights Reserved.

THE GOAL OF BASIC APPLICATION SECURITY IS TO FIX VULNERABILITIES AND RESPOND TO INCIDENTS QUICKLY.

- Focus on immediate response capabilities to address security incidents or vulnerabilities after they occur.
- Minimize downtime and operational impact caused by security breaches.
- Implement basic tools and practices (e.g., adhoc security scans, manual vulnerability remediation, manual reviews).

© 2025 Hackergirl. All Rights Reserved.



BASIC APPLICATION SECURITY

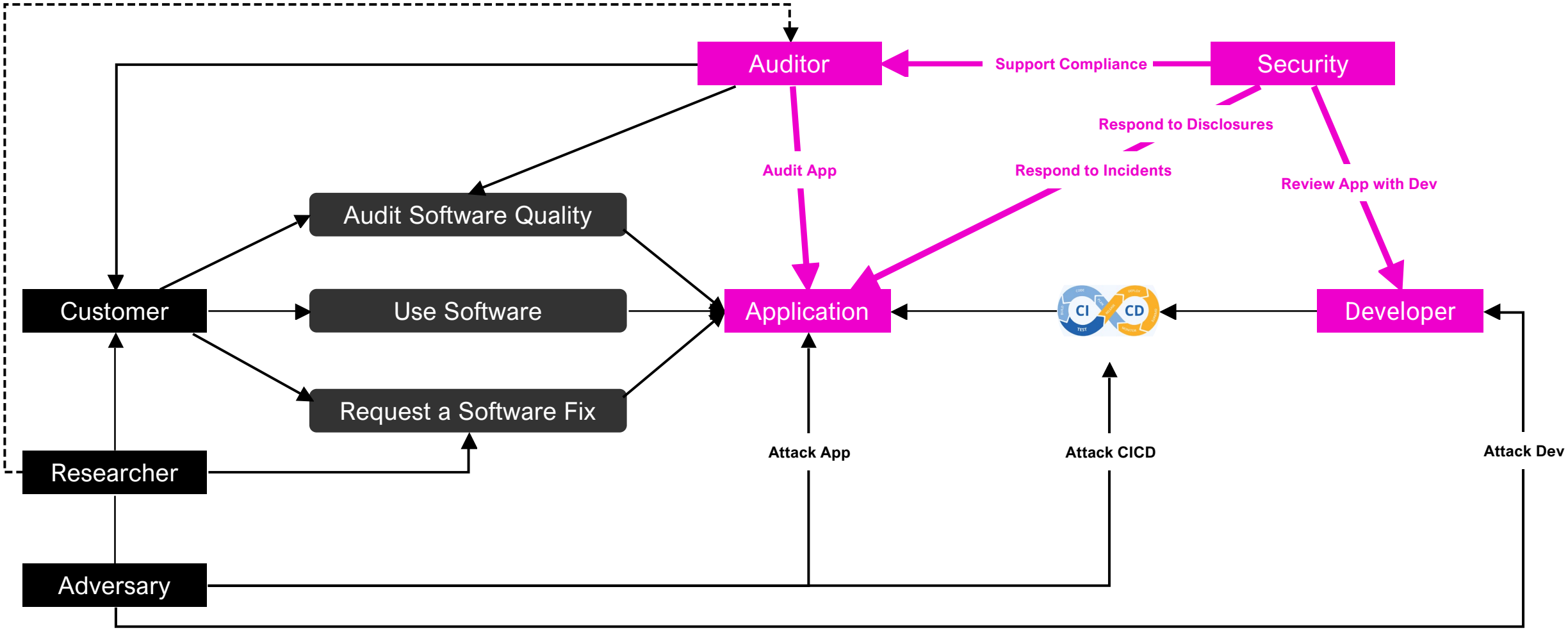
WHAT ARE KEY METRICS FOR BASIC?

- **Compliance**
  Track compliance with application requirements that support ISO and SOC2 Compliance.
- **Volume and Frequency of Escapes**
  Monitor how many and how often application security disclosures and incidents arise.
- **Mean Time to Respond**
  Measure the time taken to identify, contain, and resolve application security incidents.
- **Fix Rate**
  Track the average time taken to fix known application security vulnerabilities after they are identified.
- **Negative Impact**
  Assess the time and cost of negative impact caused by application security incidents.

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

WHAT ARE BASIC APPSEC PROCESSES?



© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

WHAT IS APP COMPLIANCE & APP AUDIT?

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

WHAT ARE APP DISCLOSURES & INCIDENTS?

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

HOW DO I ENABLE APP AUTH & LOGGING?

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

HOW DO I REVIEW AN APP WITH DEVELOPERS?

© 2025 Hackergirl. All Rights Reserved.

BASIC APPLICATION SECURITY

HOW DO I GET STARTED WITH APP REVIEWS?

Architecture View
12 Categories

1008 - Architectural Concepts

- Audit - *(1009)*
- Authenticate Actors - *(1010)*
- Authorize Actors - *(1011)*
- Cross Cutting - *(1012)*
- Encrypt Data - *(1013)*
- Identify Actors - *(1014)*
- Limit Access - *(1015)*
- Limit Exposure - *(1016)*
- Lock Computer - *(1017)*
- Manage User Sessions - *(1018)*
- Validate Inputs - *(1019)*
- Verify Message Integrity - *(1020)*

© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

Reduce Vulnerabilities and Weaknesses

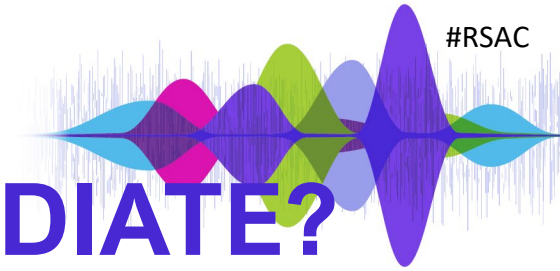
- What is the Goal of Intermediate AppSec?
- What are Key Metrics for Intermediate?
- What are Intermediate AppSec Processes?
- How do I Enable Threat Modeling?
- How do I Enable Prioritization?
- How do I Review Code?
- How do I Support SIEM, DAST, SAST & SCA?

© 2025 Hackergirl. All Rights Reserved.

THE GOAL OF INTERMEDIATE APPLICATION SECURITY IS TO REDUCE THE FREQUENCY AND SEVERITY OF APPLICATION VULNERABILITIES.

- Incorporate secure coding practices and preventive measures into the Software Development Life Cycle.
- Develop structured vulnerability management processes for tracking and prioritizing issues.
- Embed security into CI/CD pipelines to detect vulnerabilities earlier in the development process.

© 2025 Hackergirl. All Rights Reserved.



INTERMEDIATE APPLICATION SECURITY

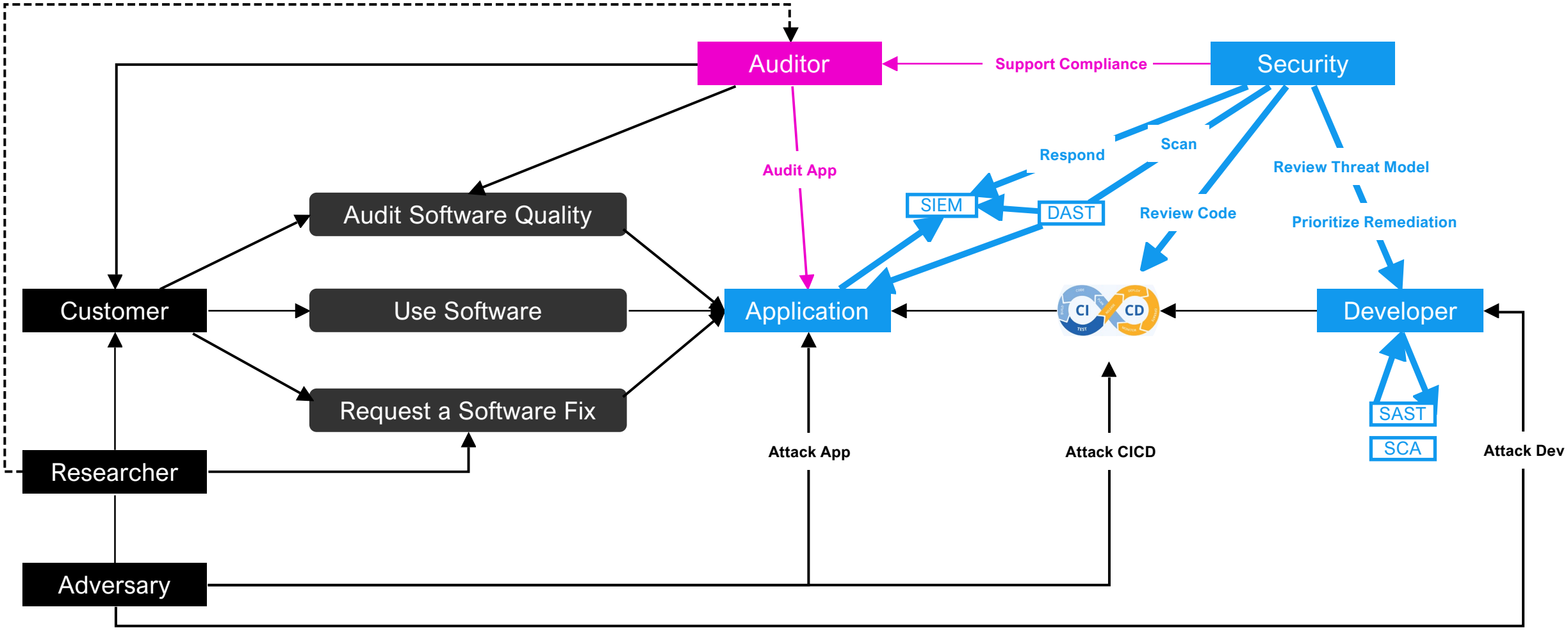
WHAT ARE KEY METRICS FOR INTERMEDIATE?

- **Frequency of Security Testing**
  Monitor how often security scans (e.g., SAST, DAST, penetration tests) are conducted during development cycles.
- **Threat Modeling Coverage**
  Measure the percentage of systems or applications analyzed for threats before deployment.
- **Improved Detection**
  Assess the increase in vulnerabilities detected earlier in the development cycle compared to post-release.
- **Secure Code Adoption**
  Track the percentage of codebases adhering to secure coding guidelines (e.g., validated inputs, proper authentication mechanisms).
- **Severity Reduction Rate**
  Evaluate the decrease in the severity of vulnerabilities over time (e.g., percentage of critical vulnerabilities mitigated).

© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

WHAT ARE INTERMEDIATE APPSEC PROCESSES?



© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

HOW DO I ENABLE THREAT MODELING?

STRIDE

PASTA

HTMM

LINDDUN

TRIKE

VAST

QTMM

DIAMOND

ATT&CK

PERSONA NON GRATA

ATTACK TREE

SECURITY CARDS

© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

HOW DO I ENABLE PRIORITIZATION?

CISA Known Exploited Vulnerabilities Catalog

CWE

EPSS
Exploit Prediction Scoring System

CVSS
Characterizing and Scoring Vulnerabilities

© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

HOW DO I REVIEW CODE?

Software View
22 Categories

Expand All | Collapse All

1400 - Comprehensive Categorization for Software Assurance Trends

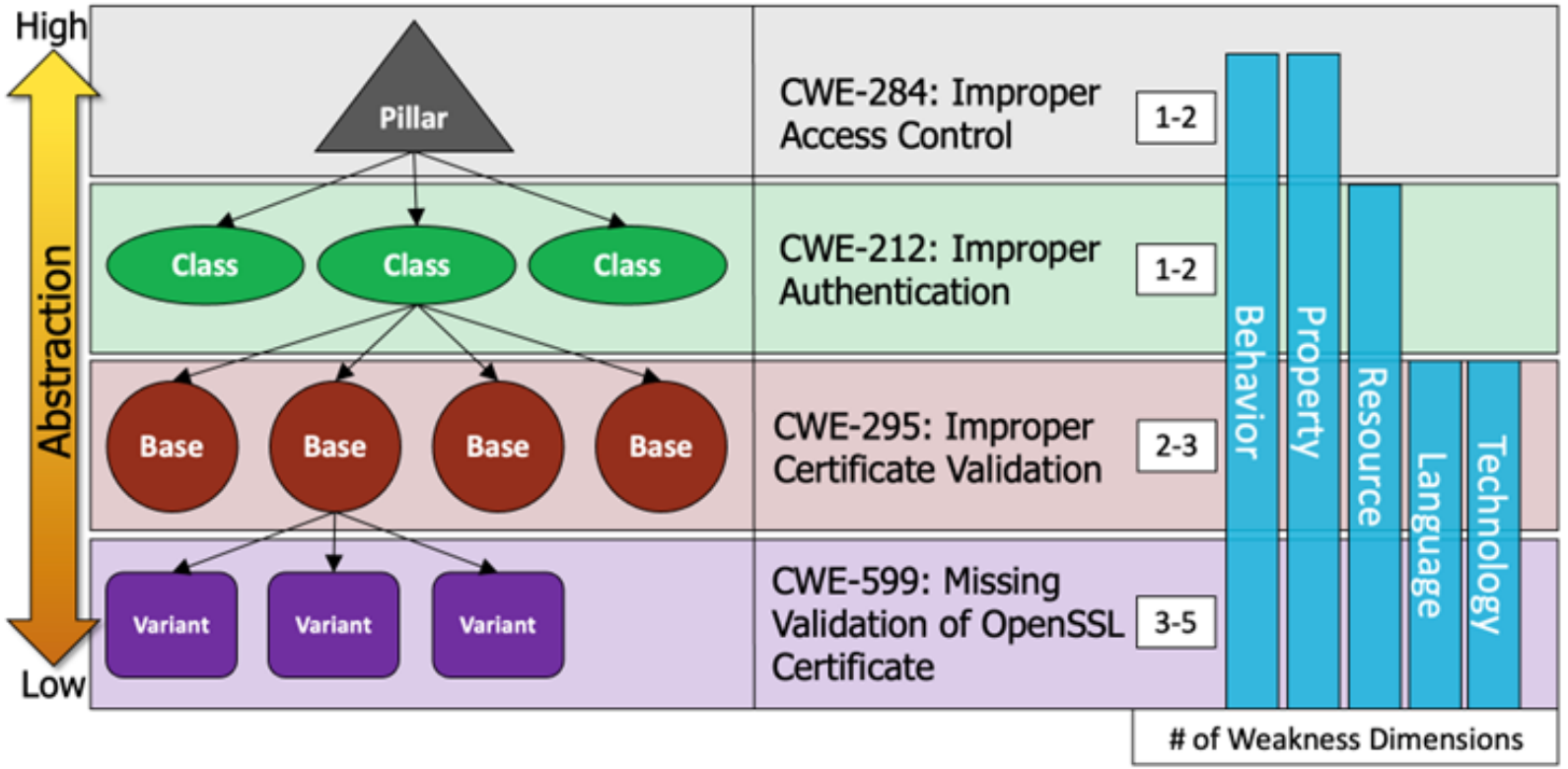
- Comprehensive Categorization: Access Control - *(1396)*
- Comprehensive Categorization: Comparison - *(1397)*
- Comprehensive Categorization: Component Interaction - *(1398)*
- Comprehensive Categorization: Concurrency - *(1401)*
- Comprehensive Categorization: Encryption - *(1402)*
- Comprehensive Categorization: Exposed Resource - *(1403)*
- Comprehensive Categorization: File Handling - *(1404)*
- Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions - *(1405)*
- Comprehensive Categorization: Improper Input Validation - *(1406)*
- Comprehensive Categorization: Improper Neutralization - *(1407)*
- Comprehensive Categorization: Incorrect Calculation - *(1408)*
- Comprehensive Categorization: Injection - *(1409)*
- Comprehensive Categorization: Insufficient Control Flow Management - *(1410)*
- Comprehensive Categorization: Insufficient Verification of Data Authenticity - *(1411)*
- Comprehensive Categorization: Memory Safety - *(1399)*
- Comprehensive Categorization: Poor Coding Practices - *(1412)*
- Comprehensive Categorization: Protection Mechanism Failure - *(1413)*
- Comprehensive Categorization: Randomness - *(1414)*
- Comprehensive Categorization: Resource Control - *(1415)*
- Comprehensive Categorization: Resource Lifecycle Management - *(1416)*
- Comprehensive Categorization: Sensitive Information Exposure - *(1417)*
- Comprehensive Categorization: Violation of Secure Design Principles - *(1418)*

© 2025 Hackergirl. All Rights Reserved.

INTERMEDIATE APPLICATION SECURITY

HOW DO I SUPPORT SIEM, DAST, SAST & SCA?

Weakness Mapping



© 2025 Hackergirl. All Rights Reserved.

ADVANCED APPLICATION SECURITY

Avoid the Possibility of Exploit

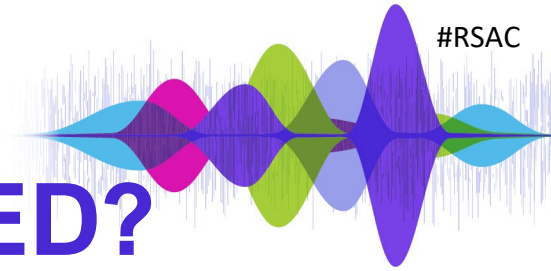
- What is the Goal of Advanced AppSec?
- What are Key Metrics for Advanced?
- What are Advanced AppSec Processes?
- What is a Paved Road Architecture?
- Why & How do I Introduce Bug Bounty?
- How can I Prevent Adversary Attacks?
- How can I Strategize Against Adversaries?

© 2025 Hackergirl. All Rights Reserved.

THE GOAL OF ADVANCED APPLICATION SECURITY IS TO AVOID EXPLOITABLE APPLICATION VULNERABILITIES.

- Focus on preventing vulnerabilities through secure design, automation, and real-time adversary intelligence.
- Establish continuous monitoring and predictive capabilities to reduce risks dynamically.
- Innovate by creating adaptive security policies and mechanisms tailored to evolving threats.

© 2025 Hackergirl. All Rights Reserved.



ADVANCED APPLICATION SECURITY

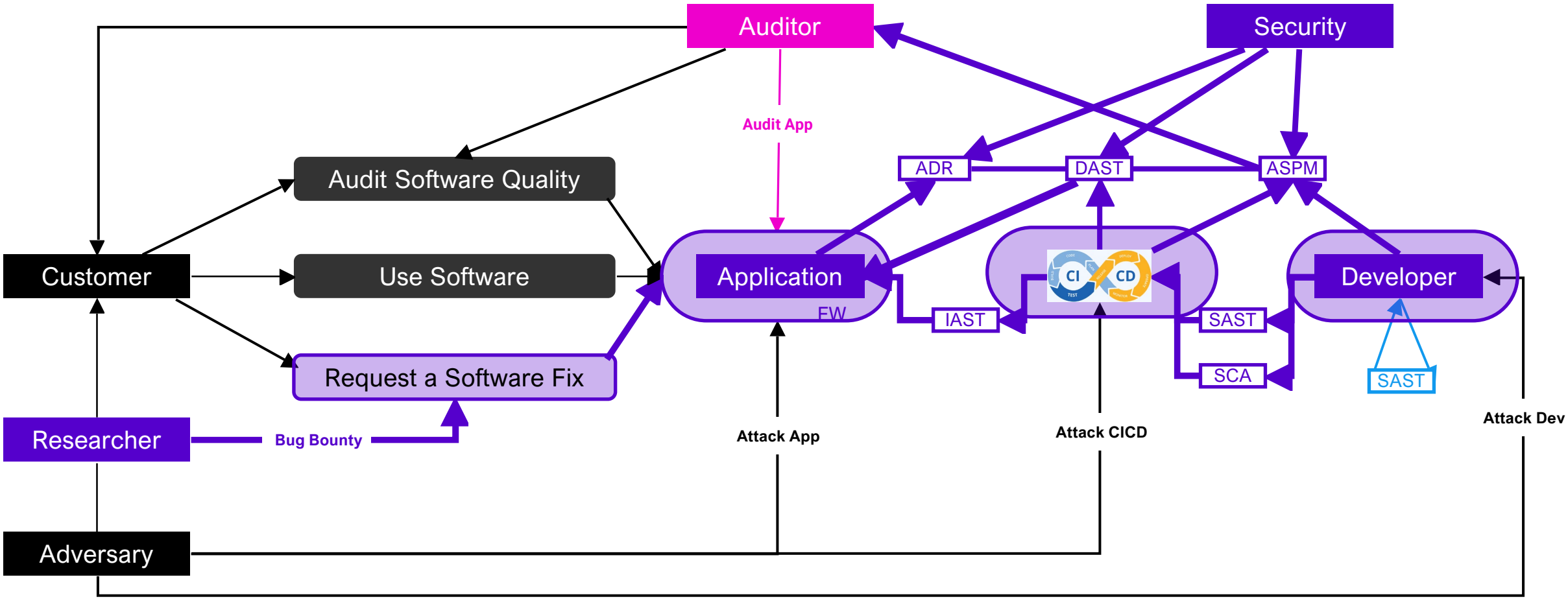
WHAT ARE KEY METRICS FOR ADVANCED?

- **Securability**
  Measure the percent of escapes vs total known exploitable opportunities and trend over time.
- **Average Adversary Dwell Time**
  Measure the length of time that an adversary spends on a particular application vs. total dwell time.
- **Time Between Incidents**
  Measure the increasing gaps between security incidents, indicating a stronger security posture.
- **Time Between Vulnerabilities**
  Measure the percentage of vulnerabilities prevented through proactive measures (e.g., secure design, automated scans in CI/CD pipelines).
- **Security Automation Coverage**
  Track the percentage of security activities fully and continuously automated (e.g., automated code scans, dependency tracking).

© 2025 Hackergirl. All Rights Reserved.

ADVANCED APPLICATION SECURITY

WHAT ARE ADVANCED APPSEC PROCESSES?



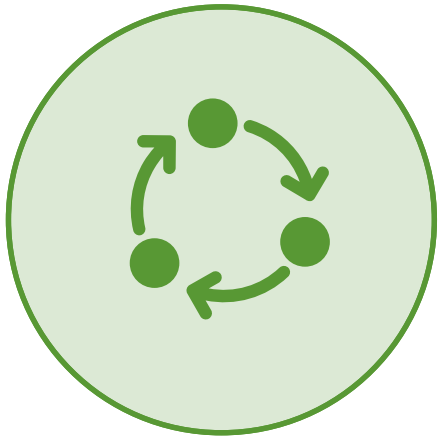
© 2025 Hackergirl. All Rights Reserved.

ADVANCED APPLICATION SECURITY

WHAT IS A PAVED ROAD ARCHITECTURE?

Gold Standards (Image, Container, Library, etc.)

Drift Detection



Closed Loop

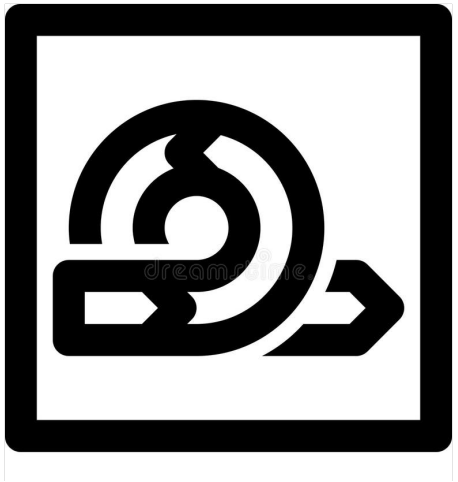
Integrated with CICD

© 2025 Hackergirl. All Rights Reserved.

ADVANCED APPLICATION SECURITY

WHY & HOW DO I INTRODUCE BUG BOUNTY?

Find a Bug Bounty Community



Define the Project

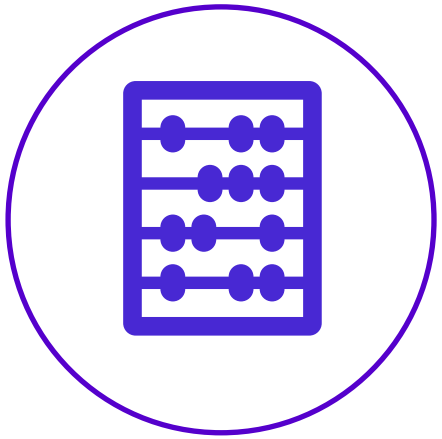
Remediate & Acknowledge Disclosed Vulnerabilities

© 2025 Hackergirl. All Rights Reserved.

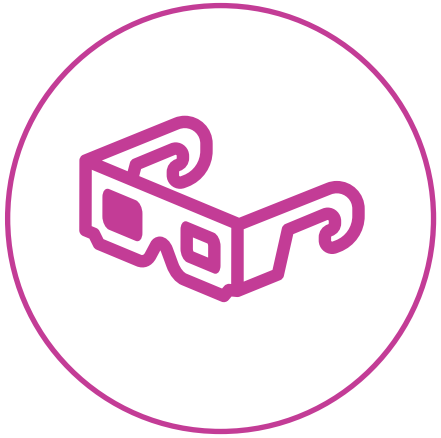
ADVANCED APPLICATION SECURITY

HOW CAN I PREVENT ADVERSARY ATTACKS?

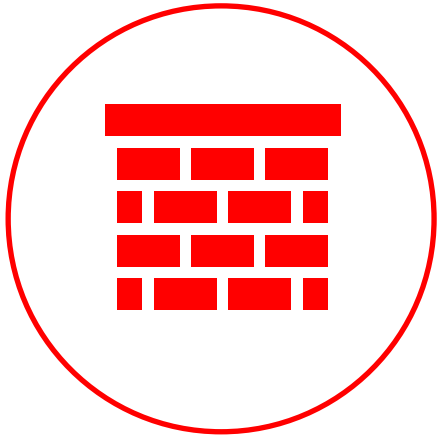
Testing & Allow Listing Components



Application Security Posture Management



Interactive Application Security Testing



Application Firewalls

Application Detection & Response

© 2025 Hackergirl. All Rights Reserved.

ADVANCED APPLICATION SECURITY

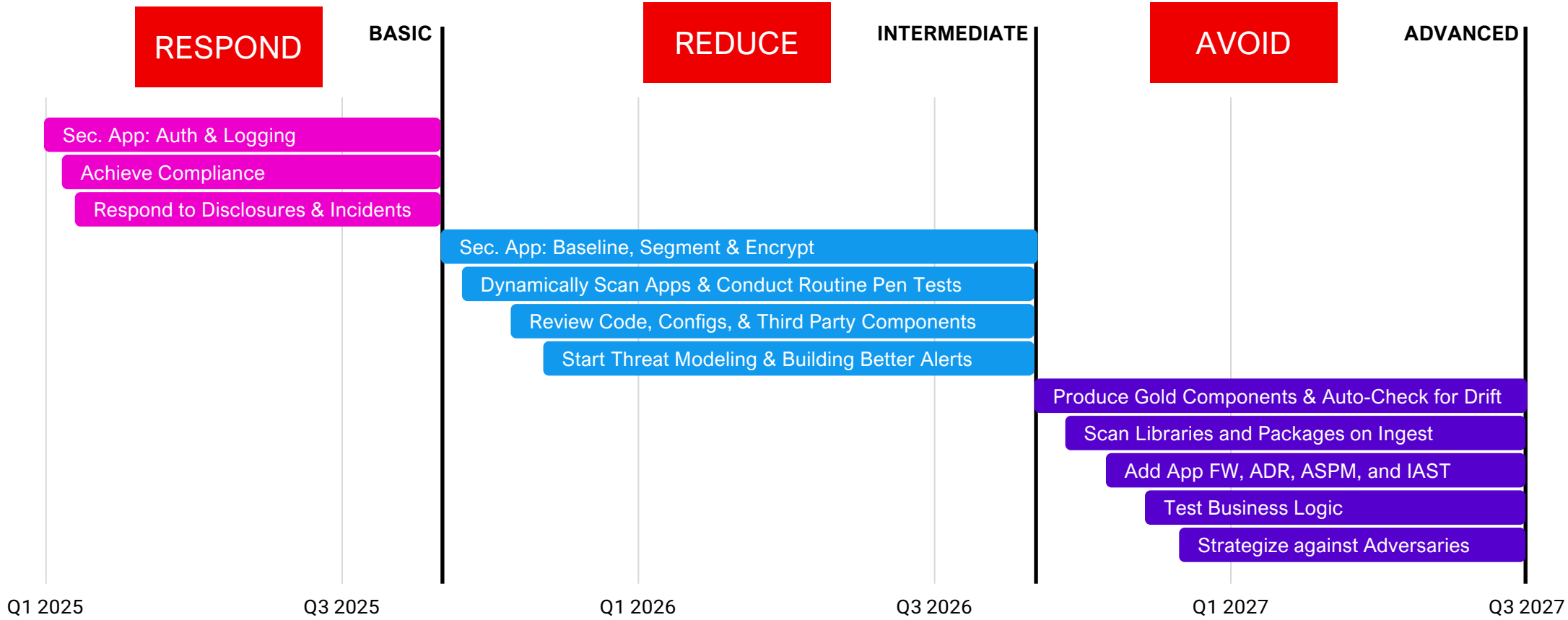
HOW CAN I STRATEGIZE AGAINST ADVERSARIES?

Class	ID	Adversary Skill	IT - Corp	IT - Cloud	BU1	BU2	BU3	Adversary Resilience 80.29%
3	A15	**Nation State**	50%	50% X	50% X	50% X	80%	X 56%
3	A14	**Mercenary Hackers**	50%	50% X	50% X	50% X	80%	X 56%
3	A13	**Supply Chain**	50%	50%	50%	50%	0%	40%
3	A12	**Fake Support**	80%	90%	100%	80%	50%	80%
3	A11	**Software Piracy**	90%	100%	85%	85%	90%	90%
2	A10	**Money Movers**	80%	95%	100%	100%	45%	84%
2	A9	**Ransomware**	80%	80%	100%	80%	100%	88%
2	A8	**Targeted Malware**	90%	90%	100%	99%	100%	96%
2	A7	**Credential Theft**	X 80%	X 75% X	80% X	100% X	100%	X 87%
2	A6	**Unauthorized Third Party**	80%	90%	100%	80%	67%	83%
1	A5	**Malware as a Service**	85%	98% X	100%	100%	100%	X 97%
1	A4	**Researchers**	100%	72%	75%	83%	82%	82%
1	A3	**Bug Bounty**	100%	75%	80%	91%	90%	87%
1	A2	**Information Gatherers**	90%	89% X	99%	97%	100%	X 95%
1	A1	**Script Kiddies**	97%	97%	25%	97%	99%	83%

© 2025 Hackergirl. All Rights Reserved.

APPLY THESE APPLICATION SECURITY FOUNDATIONS

A ROADMAP FOR GOOD TO GREAT APPSEC



© 2025 Hackergirl. All Rights Reserved.

Q&A

© 2025 Hackergirl. All Rights Reserved.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You